United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, DC 20510–6350

September 20, 1999

By Fax: 202-205-6802

The Honorable Aida Alvarez
Administrator
Small Business Administration
409 Third Street, SW
Washington, DC 20416

Dear Administrator Alvarez:

Recently, I received a report prepared by Cotton & Company on behalf of the Office of Inspector General (OIG) at the Small Business Administration (SBA/Agency) concerning the SBA's information-security efforts. The findings contained in the report are troubling.

Overall, Cotton & Company, an independent auditor, found that "the SBA has not demonstrated the senior management commitment, implemented the policies and procedures, or established the organizational structure necessary to meet Congressional and OMB requirements for information systems security."

Specifically, the audit found that the SBA has numerous information-security deficiencies including a non-effective security program, inadequate monitoring of unauthorized activities, improper access controls, excessive privileges granted to programmers and contractors, poor segregation of duties and an inadequate disaster-recovery plan, just to name some of the more egregious problems. Alarmingly, the SBA's mismanagement of information security substantially increases the risk of fraud and other abuses from within and outside the agency.

The lack of an effective security program means that fraudulent activity such as loans to phantom companies or salary checks to phantom employees or other such financial subterfuges, are difficult, if not impossible, to detect. I understand that SBA management is aware of cases involving minor fraudulent activity. The fact that such events have occurred suggests that they will continue to occur unless the SBA management moves quickly to address these problems.

Fortunately, the SBA need not invest in expensive, new computer systems to solve many of the problems outlined in the audit. What is required, however, is a strong management commitment to fix these problems. This is a management issue. With careful implementation of the recommendations, major areas of concern can and should be corrected by October 1, 2000.

The enclosed chart prepared by Cotton & Company describes the sorry state of information security at the SBA. First, it is apparent from reading the report that the Agency has done little in recent years to correct information-security controls. Some of the problems in this

year's report were cited as deficiencies identified in previous years. As the enclosed chart illustrates, some of the more serious problems governing information security at the SBA have been simply ignored.

One of the areas of greatest, continuing weakness is "Security Program, Planning and Management." The audit by Cotton & Company reveals that in every category, the SBA has no controls in place, or if there is a control, it is not fully effective. The enclosed chart indicates that in the critical area of "Security Program, Planning and Management," there are no controls in place that are effective. This is a significant exposure for an Agency with an annual budget in excess of $800 million and contingent liabilities exceeding $42 billion.

As the Chairman of the Senate Committee with oversight responsibility for the SBA, I firmly believe that you must take specific actions to correct this state of affairs. Because this issue has such far reaching and potentially disastrous implications, I intend to pay particularly close attention to your response to this report and will continue to do so until the SBA has implemented the recommendations set out in the report to the satisfaction of the SBA OIG and its independent auditors. I believe it is incumbent on you, as SBA Administrator, to set forth clear direction that this work has the highest priority at the SBA, so major improvements will be implemented before the end of FY 2000. The SBA cannot afford to allow these significant computer problems to fester and become a greater risk to the Agency and American taxpayers.

So that I am kept completely informed of the SBA's actions in this regard, please provide me with a report every thirty (30) days detailing the progress your agency is making to implement fully the recommendations set forth by the SBA OIG and Cotton & Company. I would appreciate receiving this request on the first Wednesday of each month beginning December 1, 1999. In addition, I would appreciate receiving an outline of your initial plan to take corrective action within ten (10) business days from the date of this letter.

Thank you for your prompt attention to this important matter. Please contact Paul Cooksey or Paul Conlon of the Committee staff at 202-224-5175 should you have any questions regarding this letter.

Sincerely,

Christopher Bond
Chairman

Enclosure

Attachment 1

FY 1998 CFO AUDIT – INFORMATION SYSTEMS CONTROLS REVIEW	SYSTEM					
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	*(FOIA Deletions)*					
SECURITY PROGRAM, PLANNING AND MANAGEMENT						
Risks are periodically assessed.	2	2	2	3	2	3
Security program is documented.	2	2	2	2	2	2
Security management structure is in place and responsibilities assigned.	2	2	2	2	2	2
A personnel security policy is established.	2	2	2	2	2	2
A security monitoring program is established.	2	2	2	2	2	3
ACCESS CONTROLS						
Information is properly classified.	1	2	1	1	3	3
User access and privileges are authorized.	2	2	2	2	2	2
Physical and logical controls prevent and detect unauthorized activities.	2	2	1	2	1	3
Apparent unauthorized activities are monitored and investigated.	3	2	2	2	1	3
APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL						
Program modifications are documented, reviewed, tested, and approved.	1	1	4	3	4	3
Program changes are documented, reviewed, tested, and approved before releasing to production.	1	1	4	3	4	3
Movement of programs in and out of libraries is authorized.	1	1	4	3	4	2
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	2	3	2	3	3	4
System access is monitored.	3	3	3	3	3	3
Changes to system are authorized and documented.	1	2	1	2	1	2
SEGREGATION OF DUTIES CONTROLS						
Incompatible duties are identified.	2	2	2	3	4	2
Segregation of duties is enforced through access controls.	2	2	2	3	4	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	2	2	2	3	4	2
SERVICE CONTINUITY CONTROLS						
Critical data and resources for recovery and establishment of emergency processing procedures and identified.	2	2	3	2	2	2
Procedures exist for effective backup and offsite storage of data and application and system software.	1	2	2	2	2	2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	1	3	4	2	2	3

LEGEND

1. Control in place and effective. 2. Control in place but not fully effective. 3. Control not in place. 4. Control not tested.

[1] GAO reported that "Information is FMS's systems is at significant risk because of serious general control weaknesses." (GAO/AIMD-99-10, *Financial Management Service: Areas for Improvement in Computer Controls)*